SMB署名を使用したネットワークセキュリティの強化

ONTAP 9

NetApp
February 12, 2026

目次

SMB署名を使用したネットワーク セキュリティの強化

ONTAP SMB署名を使用してネットワーク セキュリティを強化する方法について学習します

SMB署名は、リプレイ攻撃を防ぐことで、SMBサーバとクライアント間のネットワークトラフィックの侵害を防止します。デフォルトでは、ONTAPはクライアントからの要求に応じてSMB署名をサポートします。オプションで、ストレージ管理者はSMBサーバでSMB署名を必須にするように設定できます。

署名ポリシーがONTAP SMBサーバとの通信にどのように影響するかを学びます

CIFSサーバーのSMB署名セキュリティ設定に加えて、Windowsクライアント上の2つのSMB署名ポリシーが、クライアントとCIFSサーバー間の通信のデジタル署名を制御します。ビジネス要件に合った設定を構成できます。

クライアント SMB ポリシーは、Windows のローカル セキュリティ ポリシー設定によって制御されます。これらの設定は、Microsoft Management Console（MMC）または Active Directory GPO を使用して構成されます。クライアント SMB 署名とセキュリティの問題の詳細については、Microsoft Windows のドキュメントを参照してください。

Microsoft クライアント上の 2 つの SMB 署名ポリシーについて説明します：

- `Microsoft network client: Digitally sign communications (if server agrees)`

  この設定は、クライアントのSMB署名機能を有効にするかどうかを制御します。デフォルトでは有効になっています。クライアントでこの設定が無効になっている場合、CIFSサーバとのクライアント通信は、CIFSサーバのSMB署名設定に依存します。

- `Microsoft network client: Digitally sign communications (always)`

  この設定は、クライアントがサーバーとの通信にSMB署名を必要とするかどうかを制御します。デフォルトでは無効になっています。クライアントでこの設定が無効になっている場合、SMB署名の動作は `Microsoft network client: Digitally sign communications (if server agrees)`のポリシー設定とCIFSサーバーの設定に基づいて行われます。

> ⓘ 環境にSMB署名を必要とするように設定されたWindowsクライアントが含まれている場合は、CIFSサーバーでSMB署名を有効にする必要があります。有効にしないと、CIFSサーバーはこれらのシステムにデータを提供できません。

クライアントとCIFSサーバの実質的なSMB署名設定は、SMBセッションでSMB 1.0が使用されるかSMB 2.x以降が使用されるかによって異なります。

次の表に、セッションでSMB 1.0が使用される場合のSMB署名の動作を示します。

クライアント	**ONTAP—**署名は不要	**ONTAP—**署名が必要です
署名は無効になっており、必要ありません	署名なし	署名される
署名が有効で必須ではありません	署名なし	署名される
署名が無効になっていますが必須です	署名される	署名される
署名が有効で必須	署名される	署名される

古いバージョンのWindowsのSMB 1クライアントや一部のWindows以外のSMB 1クライアントでは、クライアントでは署名が無効になっていてCIFSサーバでは必要な場合、接続に失敗することがあります。

次の表に、セッションでSMB 2.xまたはSMB 3.0が使用される場合のSMB署名の動作を示します。

SMB 2.x および SMB 3.0 クライアントでは、SMB 署名は常に有効です。無効にすることはできません。

クライアント	**ONTAP—**署名は不要	**ONTAP—**署名が必要です
署名は不要です	署名なし	署名される
署名が必要です	署名される	署名される

次の表は、Microsoft クライアントおよびサーバーの SMB 署名のデフォルトの動作をまとめたものです：

プロトコル	ハッシュアルゴリズム	有効化/無効化できます	必須にできる/必須にしないことができる	クライアントのデフォルト	サーバーのデフォルト	**DC**デフォルト
SMB 1.0	MD5	はい	はい	有効（必須ではありません）	無効（必須ではありません）	必須
SMB 2.x	HMAC SHA-256	いいえ	はい	不要	不要	必須
SMB 3.0	AES-CMAC。	いいえ	はい	不要	不要	必須

Microsoftは、 `Digitally sign communications (if client agrees)`または `Digitally sign communications (if server agrees)`グループポリシー設定の使用を推奨しなくなりました。Microsoftは、 `EnableSecuritySignature`レジストリ設定の使用も推奨しなくなりました。これらのオプションはSMB 1の動作にのみ影響し、 `Digitally sign communications (always)`グループポリシー設定または `RequireSecuritySignature`レジストリ設定で置き換えることができます。Microsoftブログからも詳細情報を入手できます。http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx[SMB署名の基礎（SMB1とSMB2の両方をカバー）]

ONTAP SMB署名のパフォーマンスへの影響について学ぶ

SMBセッションでSMB署名を使用すると、SMBとWindowsクライアント間のすべての通信でパフォーマンスが低下し、クライアントとサーバ（SMBサーバを含むSVMを実行中のクラスタ ノード）の両方が影響を受けます。

パフォーマンスへの影響は、ネットワーク トラフィックの量に変化がないにもかかわらずクライアントとサーバ両方のCPU使用率が増加する形で表れます。

その程度は、実行しているONTAP 9のバージョンによって異なります。ONTAP 9.7以降では、新しい暗号化オフロード アルゴリズムによって署名済みSMBトラフィックのパフォーマンスを向上させることができます。SMB署名オフロードは、SMB署名が有効になっている場合はデフォルトで有効になります。

SMB署名のパフォーマンス向上には、AES-NIオフロード機能が必要です。ご使用のプラットフォームでAES-NIオフロードがサポートされていることを確認するには、Hardware Universe（HWU）を参照してください。

SMBバージョン3.11を使用できる場合は、より高速なGCMアルゴリズムがサポートされるため、さらなるパフォーマンスの向上が可能です。

ネットワーク、ONTAP 9のバージョン、SMBのバージョン、およびSVMの実装方法に応じてSMB署名のパフォーマンスへの影響は大幅に変わってくるため、検証するためには使用しているネットワーク環境でテストを実施する必要があります。

ほとんどのWindowsクライアントは、サーバでSMB署名が有効になっている場合は、SMB署名をデフォルトでネゴシエートします。Windowsクライアントの一部でSMB保護が必要で、SMB署名がパフォーマンスの問題を引き起こしている場合は、リプレイ アタックからの保護を必要としないWindowsクライアントに対してSMB署名を無効にすることができます。WindowsクライアントでのSMB署名の無効化については、Microsoft Windowsのマニュアルを参照してください。

ONTAP SMB署名設定の推奨事項

SMBクライアントとCIFSサーバの間のSMB署名の動作は、セキュリティ要件に応じて設定することができます。CIFSサーバでのSMB署名の設定は、セキュリティ要件の内容によって異なります。

SMB署名は、クライアントとCIFSサーバのどちらでも設定できます。SMB署名を設定する際の推奨事項を次に示します。

状況	推奨事項...
クライアントとサーバの間の通信のセキュリティを強化する	クライアントで `Require Option (Sign always)`セキュリティ設定を有効にして、SMB 署名を必須にします。
特定のStorage Virtual Machine（SVM）へのすべてのSMBトラフィックに署名する	セキュリティ設定でSMB署名を必須にするように設定して、CIFSサーバでSMB署名を必須にします。

Windowsクライアントのセキュリティ設定の詳細については、Microsoftのドキュメントを参照してください。

複数のデータLIFに対するONTAP SMB署名設定について学習します

SMB サーバーで必要な SMB 署名を有効または無効にする場合は、SVM の複数のデータ LIF 構成に関するガイドラインに注意する必要があります。

SMBサーバを設定する場合、複数のデータLIFが設定されている場合があります。その場合、DNSサーバには、CIFSサーバの `A`レコード エントリが複数含まれます。これらのレコード エントリはすべて同じSMBサーバ ホスト名を使用していますが、IPアドレスはそれぞれ異なります。たとえば、2つのデータLIFが設定されているSMBサーバの場合、DNS `A`レコード エントリは次のようになります：

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

通常の動作では、必要なSMB署名設定を変更すると、クライアントからの新規接続のみがSMB署名設定の変更の影響を受けます。ただし、この動作には例外があります。クライアントが既に共有に接続しており、設定変更後に元の接続を維持しながら、同じ共有への新規接続を作成する場合があります。この場合、新規接続と既存のSMB接続の両方に新しいSMB署名要件が適用されます。

次の例を考えてみましょう。

1. Client1 は、パス `O:\`を使用して、必要な SMB 署名なしで共有に接続します。
2. ストレージ管理者は、SMB 署名を要求するように SMB サーバー構成を変更します。
3. Client1 は、パス `S:\`を使用して必要な SMB 署名で同じ共有に接続します（パス `O:\`を使用した接続を維持しながら）。
4. その結果、 `O:\`ドライブと `S:\`ドライブの両方を介してデータにアクセスするときに SMB 署名が使用されます。

受信SMBトラフィック用のONTAP署名を設定する

SMBメッセージへのクライアントによる署名を強制するには、SMB署名要求を有効にします。有効にすると、ONTAPは有効な署名のあるSMBメッセージのみを受け入れます。SMB署名を許可するが要求しない場合は、SMB署名要求を無効にできます。

タスク概要

デフォルトでは、SMB署名要求は無効になっています。SMB署名要求は随時有効または無効にできます。

次の状況では、SMB署名はデフォルトで無効になりません。

1. SMB署名要求が有効になっており、クラスタがSMB署名をサポートしていないバージョンのONTAPにリバートされた。
2. その後、クラスタがSMB署名をサポートするバージョンのONTAPにアップグレードされた。

このような場合は、サポートされているバージョンのONTAPで最初に行われたSMB署名の設定が、リバートとその後のアップグレードを通して維持されます。

Storage Virtual Machine（SVM）のディザスタ リカバリ関係を設定する場合、 `snapmirror create`コマンドの `-identity-preserve`オプションに選択した値によって、デスティネーションSVMにレプリケートされる設定の詳細が決まります。

`-identity-preserve`オプションを `true`（ID保持）に設定すると、SMB署名のセキュリティ設定が宛先に複製されます。

`-identity-preserve`オプションを `false`（ID保持なし）に設定した場合、SMB署名セキュリティ設定はデスティネーションにレプリケートされません。この場合、デスティネーションのCIFSサーバ セキュリティ設定はデフォルト値に設定されます。ソースSVMでSMB署名要求を有効にしている場合は、デスティネーションSVMでも手動でSMB署名要求を有効にする必要があります。

手順

1. 次のいずれかを実行します。

必須の**SMB**署名を有効にする場合...	コマンドを入力してください...
有効	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required true`
無効	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required false`

2. 次のコマンドの出力の `Is Signing Required`フィールドの値が目的の値に設定されているかどうかを確認して、必要なSMB署名が有効か無効かを確認します。 `vserver cifs security show -vserver` *`vserver_name`* `-fields is-signing-required`

例

次の例は、SVM vs1でSMB署名要求を有効にします。

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required
true

cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-
required
vserver  is-signing-required
-------- --------------------
vs1      true
```

暗号化設定の変更点は、新しい接続に対して有効になります。既存の接続は影響を受けません。

関連情報

- "snapmirror create"

ONTAPSMBセッションが署名されているかどうかを確認する

CIFSサーバで接続中のSMBセッションに関する情報を表示できます。この情報を使用して、SMBセッションが署名されているかどうかを確認できます。これは、必要なセキュリティ設定を使用してSMBクライアント セッションが接続されているかどうかを確認する場合に役立ちます。

手順

1. 次のいずれかを実行します。

...に関する情報を表示する場合	コマンドを入力してください...
指定したStorage Virtual Machine（SVM）上の署名されたすべてのセッション	`vserver cifs session show -vserver vserver_name -is-session-signed true`
SVM上の指定したセッションIDを持つ署名されたセッションの詳細	`vserver cifs session show -vserver vserver_name -session-id integer -instance`

例

次のコマンドは、SVM vs1上の署名済みセッションに関するセッション情報を表示します。デフォルトのサマリー出力には、「`Is Session Signed`」出力フィールドは表示されません：

```
cluster1::> vserver cifs session show -vserver vs1 -is-session-signed true
Node:    node1
Vserver: vs1
Connection Session                                      Open          Idle
ID         ID      Workstation      Windows User    Files         Time
---------- ------- ---------------- ------------- ------- ------------
3151272279 1       10.1.1.1         DOMAIN\joe          2          23s
```

次のコマンドは、セッションID 2のSMBセッションに関する、セッションが署名されているかどうかを含む詳細なセッション情報を表示します。

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                 Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   UNIX User: pcuser
                Open Shares: 1
                 Open Files: 1
                 Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

関連情報

SMB署名済みセッションの統計の監視

ONTAP SMB署名セッション統計を監視する

SMBセッションの統計を監視し、確立されたセッションのうち、署名されたセッションと署名されていないセッションを区別できます。

タスク概要

`statistics`上級権限レベルのコマンドは、署名済みSMBセッションの数を監視するために使用できる `signed_sessions`カウンタを提供します。
`signed_sessions`カウンタは、以下の統計オブジェクトで使用できます：

- `cifs`を使用すると、すべての SMB セッションの SMB 署名を監視できます。
- `smb1`を使用すると、SMB 1.0 セッションの SMB 署名を監視できます。
- `smb2`では、SMB 2.x および SMB 3.0 セッションの SMB 署名を監視できます。

  `smb2`オブジェクトの出力には SMB 3.0 統計が含まれます。

署名されたセッションの数とセッションの合計数を比較する場合は、 `signed_sessions`カウンターの出力と`established_sessions`カウンターの出力を比較できます。

データを取得して表示するには、統計サンプルの収集を開始する必要があります。データ収集を停止しなければ、サンプルからデータを表示できます。データ収集を停止すると、固定のサンプル データが表示されます。データ収集を停止しなければ、以前のクエリとの比較に使用できる更新されたデータを入手できます。この比較は、パフォーマンスの傾向を確認するのに役立ちます。

手順

1. 権限レベルを詳細に設定します：+ `set -privilege advanced`
2. データ収集を開始する：+ `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   `-sample-id`パラメータを指定しない場合、コマンドはサンプル識別子を生成し、このサンプルをCLIセッションのデフォルト サンプルとして定義します。 `-sample-id`の値はテキスト文字列です。同じCLIセッション中にこのコマンドを実行し、 `-sample-id`パラメータを指定しない場合、コマンドは以前のデフォルト サンプルを上書きします。

   オプションで、統計情報を収集するノードを指定できます。ノードを指定しない場合、サンプルは、クラスタ内のすべてのノードについて統計情報を収集します。

   `statistics start`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/statistics-start.html["ONTAPコマンド リファレンス"^]を参照してください。

3. `statistics stop`コマンドを使用して、サンプルのデータ収集を停止します。

`statistics stop`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/statistics-stop.html["ONTAPコマンド リファレンス"^]を参照してください。

4. 次のコマンドによりSMB署名統計を表示します。

...の情報を表示する場合は	入力する内容
署名されたセッション	`show -sample-id sample_ID -counter signed_sessions
node_name [-node *node_name*]`	署名されたセッションおよび確立されたセッション
`show -sample-id *sample_ID* -counter signed_sessions	established_sessions

1 つのノードのみの情報を表示する場合は、オプションの `-node`パラメータを指定します。

`statistics show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/statistics-show.html["ONTAPコマンド リファレンス"^]をご覧ください。

5. admin権限レベルに戻ります：+ `set -privilege admin`

例

次の例は、「vs1」というStorage Virtual Machine（SVM）について、SMB 2.xとSMB 3.0のそれぞれの署名統計情報を監視する方法を示します。

次のコマンドは、advanced権限レベルへの変更を行います。

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

次のコマンドは、新しいサンプルのデータ収集を開始します。

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample
-vserver vs1
Statistics collection is being started for Sample-id: smbsigning_sample
```

次のコマンドは、サンプルのデータ収集を停止します。

```
cluster1::*> statistics stop -sample-id smbsigning_sample
Statistics collection is being stopped for Sample-id: smbsigning_sample
```

次のコマンドでは、ノードが署名、確立した各SMBセッションをサンプルから表示します。

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|established_sessions|node_name

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:03:04
Cluster: cluster1

    Counter                                                  Value
    -------------------------------- ------------------------
    established_sessions                                         0
    node_name                                                node1
    signed_sessions                                              0
    established_sessions                                         1
    node_name                                                node2
    signed_sessions                                              1
    established_sessions                                         0
    node_name                                                node3
    signed_sessions                                              0
    established_sessions                                         0
    node_name                                                node4
    signed_sessions                                              0
```

次のコマンドでは、ノード2が署名したSMBセッションをサンプルから表示します。

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|node_name -node node2

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:22:43
Cluster: cluster1

    Counter                                                  Value
    -------------------------------- ------------------------
    node_name                                                node2
    signed_sessions                                              1
```

次のコマンドで、admin権限レベルに戻ります。

```
cluster1::*> set -privilege admin
```

関連情報

- SMBセッションが署名されているかどうかの確認
- "パフォーマンスの監視と管理 - 概要"

著作権に関する情報

商標に関する情報